Sign in

Google

Web Images Video News Maps more »

operation code and decryption key Search Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web Results **1 - 10** of about **1,070,000** for **operation code and decryption key**. (**0.38** seconds)

Encryption - Wikipedia, the free encyclopedia
The **operation** of a cipher usually depends on a piece of auxiliary information, ... By whether the same **key** is used for both encryption and **decryption** ...
en.wikipedia.org/wiki/Encryption - 40k - Apr 3, 2007 - Cached - Similar pages

[PDF] Express Letter Triple Encryption Packaging Scheme for Preserving ...
File Format: PDF/Adobe Acrobat
information and **decryption key** K2, (b) without **decryption key** K2, and. (c) with wrong harm **code. key**, namely, by doing EX-OR **operations** of the first encoded ...
jjap.ipap.jp/link?JJAP/41/L305/ - Similar pages

Key management for encryption/**decryption** systems - Patent 4281216
In a data encryption/**decryption** system providing for security of data ... These **codes** identify the **operation** to be performed by the **key** generator. ...
www.freepatentsonline.com/4281216.html - 54k - Cached - Similar pages

Comments on FC00 paper
>It would not need to be "public" **key** and could be a pure "secret" >**key** cryptographic **operation**. It is true that this **code** could use a single-**key** system ...
www.eros-os.org/pipermail/e-lang/1999-November/002930.html - 9k - Cached - Similar pages

Download details: Visual Basic .NET **Code** Sample: Encrypt and ...
Anyone that has the **key** can **decrypt** the data, which makes protection of the **key** vital. ... Supported **Operating** Systems: Windows 2000; Windows NT; Windows XP ...
www.microsoft.com/downloads/details.aspx?FamilyID=83f3c2d1-ced6-473e-9cbe-723ca1f0267d&displaylang=en - 30k - Cached - Similar pages

CD-Cops -- CD-ROM copy protection of the highest level. - CD-Cops ...
For most copy-protection use the **decryption key** is by no means public, it is supposed to be guarded well inside secure **code**. If a pirate should find the ...
www.linkdata.com/intruder.htm - 17k - Cached - Similar pages

Encrypt <--> **Decrypt** Data with C# - The **Code** Project - C# Programming
A good encryption and **decryption code** is easily findable in the Internet and even in ... **Key** = keyArray; //mode of **operation**. there are other 4 modes. ...
www.**code**project.com/useritems/Cryptography.asp - 35k - Cached - Similar pages

Introduction to **Code** Signing (Windows IETechCol)
Furthermore, the **decryption key** cannot be reasonably calculated from the encryption ... In order to perform a **code** signing **operation**, both private **key** and ...
msdn.microsoft.com/workshop/security/auth**code**/intro_authenti**code**.asp - 29k - Cached - Similar pages

[PDF] 4.3 The Command Descriptor Block (CDB)
File Format: PDF/Adobe Acrobat - View as HTML
The general structure of the **operation code** and control byte are defined in SAM-2. ... The value also indicates which encryption **key** to use for **decryption**. ...
www.t10.org/ftp/t10/document.00/00-269r2.pdf - Similar pages

[PDF] Secret Key Management Based on Variable Authentication **Code** in UPT ...
File Format: PDF/Adobe Acrobat
operation code (OP) agreed between the **key** server and a plurality of ... also uses rSD as the **key** to **decrypt** the message, checks if the message has the ...
ieeexplore.ieee.org/iel4/5969/16009/00743404.pdf?tp=&arnumber=743404&isnumber=16009 - Similar pages

Sign in

Google

Web Images Video News Maps more »

operation code and decryption key Search Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web Results **11** - **20** of about **1,070,000** for **operation code and decryption key**. (**0.12** seconds)

Code Signing Certificates Buy from SSL Certificate Authority
Furthermore, the **decryption key** cannot be reasonably calculated from the ... e-commerce **operations** by Establishing Trust™ initiatives for e-Business, ...
www.instantssl.com/**code**-signing/ - 24k - Cached - Similar pages

[PDF] CSE380 - **Operating** Systems
File Format: PDF/Adobe Acrobat - View as HTML
Write the actual **code** for the remote service. (in a .x file). – Select a service id for your service ... can't figure out **decryption key** from encryption **key** ...
www.crypto.com/courses/fall06/cse380/20061128.pdf - Similar pages

> [PDF] CSE380 - **Operating** Systems
> File Format: PDF/Adobe Acrobat - View as HTML
> electronic **code** book mode. • Sender & receiver agree on secret **key**. – needs to be unpredictable, ... can't figure out **decryption key** from encryption **key** ...
> www.crypto.com/courses/fall06/cse380/20061130.pdf - Similar pages
> [More results from www.crypto.com]

[PDF] Page 1 Security Policy Ensuredmail (9/25/2000) Revised 2/19/01 1.0 ...
File Format: PDF/Adobe Acrobat - View as HTML
Key management. Password entry. User. Cryptographic **operations**. Encryption/**Decryption**. User. Self test (automatic). Software integrity check ...
csrc.nist.gov/cryptval/140-1/140sp/140sp140.pdf - Similar pages

> CRYPTOGRAPHIC STANDARDS AND GUIDELINES: A STATUS REPORT By Elaine ...
> **Decryption** transforms the ciphertext back into plaintext using a **decryption key**. Several algorithms have been approved in FIPS for the encryption of ...
> csrc.nist.gov/publications/nistbul/itl09-02.txt - 20k - Cached - Similar pages
> [More results from csrc.nist.gov]

TCLLIB - Tcl Standard Library: des
::DES::Encrypt **Key** data ::DES::**Decrypt Key** data ::DES::Reset **Key** iv ... MODES OF **OPERATION**. Electronic **Code** Book (ECB): ECB is the basic mode of all block ...
www.ensta.fr/~diam/tcl/online/tcllib/des.html - 11k - Cached - Similar pages

Mailing list archives
+Once you checkout a source tree, all CVS **operations** in that source tree +do ... This +stores the private **key** in <**code**>$HOME/.ssh/identity</**code**> and the ...
mail-archives.apache.org/mod_mbox/jakarta-site-cvs/200107.mbox/%3C20010705225541.97661.qmail@apache.org%3E - 10k - Cached - Similar pages

Crytographic tools for Visual Basic
So we need a one way **operation** where you can calculate the encryption **key** from the **decryption key**, but you cannot calculate the **decryption key** from the ...
www.echeque.com/Kong/tools.htm - 14k - Cached - Similar pages

Microsoft Office 2000 Resource Kit
In multitasking **operating** systems, allows more than one thread or process ... virtual **key code** Hardware-independent number that uniquely identifies a **key** on ...
msdn2.microsoft.com/en-us/library/aa833098(office.10).aspx - 47k - Cached - Similar pages

MidNyte 'Introduction to Encryption, Part I' (VX heavens)
You might want to research RDK (Random **Decryption Key**) and RDA (Random ... encrypt and **decrypt** the **code** sections, as the **operations** chosen are reversible. ...
vx.netlux.org/lib/vmn04.html - 16k - Cached - Similar pages

Sign in

Google

Web Images Video News Maps more »

operation code and decryption key Search Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web Results **21** - **30** of about **1,070,000** for **operation code and decryption key**. (**0.19** seconds)

Symmetric **Key** Cryptography
Decryption is the reverse **operation**: its input consists of the ciphertext ... a message and a **key** and outputs a so-called Message Authentication **Code** (MAC). ...
www.algorithmic-solutions.info/leda_manual/symmetric_key_cryptography.html - 18k - Cached - Similar pages

Introduction to Computing Security
and the **decryption**. P = Cd mod n. The encryption **key** consists of the pair of integers ... Undefined **operation codes** in microprocessors; Poor error checking ...
cui.unige.ch/OSG/courses/infrcom/OLD/lectures/security/security.html - 25k - Cached - Similar pages

des(n): Implementation of DES/triple-DES ... - Linux man page
::DES::**Decrypt Key** data: Decipher data using the **key**. ... MODES OF **OPERATION**. Electronic **Code** Book (ECB): ECB is the basic mode of all block ciphers. ...
www.die.net/doc/linux/man/mann/des.n.html - 12k - Cached - Similar pages

NSS and SSL Error **Codes**
All the error **codes** in the following block describe the **operation** that ... -8146, Cannot **decrypt**: **key** encryption algorithm does not match your certificate. ...
www.mozilla.org/projects/security/pki/nss/ref/ssl/sslerr.html - 88k - Cached - Similar pages

Translate Data (QC3TRNDT, Qc3TranslateData)
If the **decrypt** mode of **operation** is CFB 1-bit, the length must be specified in bits. ... Reason **code** &3. CPF9DC2 E, **Key**-encrypting algorithm context not ...
publib.boulder.ibm.com/infocenter/iseries/v5r3/topic/apis/qc3trndt.htm - 14k - Cached - Similar pages

The CSS **Decryption** Algorithm
Further insight into the **operation** of the algorithm can be obtained by ... These bytes are the **decryption key** (the player **key**) that the procedure will use ...
www.cs.cmu.edu/~dst/DeCSS/Gallery/plain-english.html - 18k - Cached - Similar pages

DVD Decrypter Version 3.5.4.0 - A User Guide - Page 3 - Digital ...
If you press 'Yes' - the program will try to use a **decryption key** from another file ... I 18:00:26 **Operation** Started! I 18:00:26 Source Device: [1:1:0] JLMS ...
forum.digital-digest.com/showthread.php?t=51575&page=3 - 50k - Cached - Similar pages

wrapping a hashed message authentication **code** hmac **key**
Decrypt the wrapped **key** in CBC mode using the 3DES KEK. ... ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of **Operation**. 1998. ...
www.ietf.org/rfc/rfc3537.txt - 17k - Cached - Similar pages

Cryptographic Papers : Basic Concepts
Generic source for Encryption, **Decryption** and **Key** Management. ... of arbitrary length, we can use one of the following techniques (or modes of **operation**): ...
www.cryptographyworld.com/concepts.htm - 23k - Cached - Similar pages

[PDF] An Instruction-Level Distributed Processor for Symmetric-**Key** ...
File Format: PDF/Adobe Acrobat
encryption and a private **key** for **decryption**. In a typical. session, a public-**key** algorithm will ... The instruction word comprises the **operation code**, slice ...
ieeexplore.ieee.org/iel5/71/30581/01411734.pdf - Similar pages

Terms used operation code and decryption code Found 70,465 of 199,787

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Network security: Analyzing network traffic to detect self-decrypting exploit code

Qinghua Zhang, Douglas S. Reeves, Peng Ning, S. Purushothaman Iyer

March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**

Publisher: ACM Press

Full text available: pdf(269.73 KB) Additional Information: full citation, abstract, references, index terms

Remotely-launched software exploits are a common way for attackers to intrude into vulnerable computer systems. As detection techniques improve, remote exploitation techniques are also evolving. Recent techniques for evasion of exploit detection include *polymorphism* (code encryption) and *meta-morphism* (code obfuscation). This paper addresses the problem of detecting in network traffic polymorphic remote exploits that are encrypted, and that self-decrypt before launching the intrusi ...

Keywords: decryption, detection, emulation, exploit code, polymorphic, static analysis

2 Implementing an untrusted operating system on trusted hardware

David Lie, Chandramohan A. Thekkath, Mark Horowitz

October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5

Publisher: ACM Press

Full text available: pdf(280.87 KB) Additional Information: full citation, abstract, references, citings, index terms

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware~---~TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM~---~a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted.Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

3 Content protection: Cell Broadband Engine™ processor security architecture and digital content protection

Kanna Shimizu, Stefan Nusser, Wilfred Plouffe, Vladimir Zbarsky, Masaharu Sakamoto, Masana Murase

October 2006 **Proceedings of the 4th ACM international workshop on Contents protection and security MCPS '06**

Publisher: ACM Press

Full text available: pdf(260.80 KB) Additional Information: full citation, abstract, references, index terms

Current content protection technologies such as those based on broadcast encryption and public-key encryption focus on the distribution and control of content. Although these technologies are effective and mathematically sound, they are susceptible to systematic attacks that utilize any underlying platform weakness, bypassing the cryptographic

strengths of the actual schemes. Thus, ensuring that the computing platform supports the cryptographic content protection layers on top is a critical issu ...

Keywords: content protection, processor architecture

4 Modeling methodology B: modeling and simulation of computer systems: Performance analysis of binary code protection

David M. Nicol, Hamed Okhravi

December 2005 **Proceedings of the 37th conference on Winter simulation WSC '05**

Publisher: Winter Simulation Conference

Full text available: pdf(159.34 KB) Additional Information: full citation, abstract, references

Software protection technology seeks to prevent unauthorized observation or use of applications. Cryptography can be used to provide such protection, but imposes a potentially significant additional computation load. This paper examines the performance impact of two software protection techniques. We develop an analytic model and validate it using a detailed discrete-event simulator applied to memory reference traces of well-known benchmark programs. We find that even though the added workload m ...

5 Student papers: FMS and FMSE encryption/decryption algorithms using flipping, mapping, and shifting operations

Peter Phuong Vo, Chau Maggie Vo

September 2006 **Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06**

Publisher: ACM Press

Full text available: pdf(65.04 KB) Additional Information: full citation, abstract, references, index terms

Cryptography is one of the most important areas in the computer industry. Encryption allows an application to secure its data from being accessed by hackers. Currently there are many industry-standard encryption/decryption algorithms including RSA, Rijndael, Blowfish [1,2], and so forth. However, they are fairly complex and require that one spend a lot of time to comprehend and implement them. This paper introduces two simple encryption/decryption algorithms that are fast and fairly secure. T ...

Keywords: encryption/decryption using flipping, mapping, shifting operations

6 Security: Hardware support for code integrity in embedded processors

Milena Milenković, Aleksandar Milenković, Emil Jovanov

September 2005 **Proceedings of the 2005 international conference on Compilers, architectures and synthesis for embedded systems CASES '05**

Publisher: ACM Press

Full text available: pdf(371.76 KB) Additional Information: full citation, abstract, references, index terms

Computer security becomes increasingly important with continual growth of the number of interconnected computing platforms. Moreover, as capabilities of embedded processors increase, the applications running on these systems also grow in size and complexity, and so does the number of security vulnerabilities. Attacks that impair code integrity by injecting and executing malicious code are one of the major security issues. This problem can be addressed at different levels, from more secure softwa ...

Keywords: attacks, code injection, code integrity

7 Hardware and Binary Modification Support for Code Pointer Protection From Buffer Overflow

Nathan Tuck, Brad Calder, George Varghese

December 2004 **Proceedings of the 37th annual IEEE/ACM International Symposium on Microarchitecture MICRO 37**

Publisher: IEEE Computer Society

Full text available: pdf(294.15 KB) Additional Information: full citation, abstract, citings

Buffer overflow vulnerabilities are currently the most prevalent security vulnerability; they are responsible for over half of the CERT advisories issued in the last three years.Since many attacks exploit buffer overflow vulnerabilities, techniques that prevent buffer overflow attacks would greatly increase the difficulty of writing a new worm. This paper

examines both software and hardware solutions for protecting code pointers from buffer overflow attacks.We first evaluate the performance over ...

8 Crypto technology: Privacy-enhanced superdistribution of layered content with trusted access control

Daniel J. T. Chong, Robert H. Deng

October 2006 **Proceedings of the ACM workshop on Digital rights management DRM '06**

Publisher: ACM Press

Full text available: pdf(226.77 KB) Additional Information: full citation, abstract, references, index terms

Traditional *superdistribution* citemori: superdistribution approaches do not address consumer privacy issues and also do not reliably prevent the malicious consumer from indiscriminately copying and redistributing the decryption keys or the decrypted content. The layered nature of common digital content can also be exploited to efficiently provide the consumer with choices over the quality of the content, allowing him/her to pay less for lower quality consumption and vice versa. This paper ...

Keywords: DRM, access control, copyrights, digital distribution, licensing, privacy, trusted computing, usage rights

9 Software engineering for security: a roadmap

Premkumar T. Devanbu, Stuart Stubblebine

May 2000 **Proceedings of the Conference on The Future of Software Engineering ICSE '00**

Publisher: ACM Press

Full text available: pdf(1.71 MB) Additional Information: full citation, references, citings, index terms

Keywords: copy protection, security, software engineering, water-marking

10 Bidirectional mobile code trust management using tamper resistant hardware

John Zachary, Richard Brooks

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available: pdf(152.99 KB) Additional Information: full citation, abstract, references, index terms

Trust management in a networked environment consists of authentication and integrity checking. In a mobile computing environment, both remote hosts and mobile code are suspect. We present a model that addresses trust negotiation between the remote host and the mobile code simultaneously. Our model uses tamper resistant hardware, public key cryptography, and one-way hash functions.

Keywords: authentication, hash functions, mobile code, tamper resistant hardware, trust management

11 Informal tool demonstrations: A tool for analyzing and detecting malicious mobile code

Akira Mori, Tomonori Izumida, Toshimi Sawada, Tadashi Inoue

May 2006 **Proceeding of the 28th international conference on Software engineering ICSE '06**

Publisher: ACM Press

Full text available: pdf(99.00 KB) Additional Information: full citation, abstract, references, index terms

We present a tool for analysis and detection of malicious mobile code such as computer viruses and internet worms based on the combined use of code simulation, static code analysis, and OS execution emulation. Unlike traditional anti-virus methods, the tool directly inspects the code and identifies commonly found malicious behaviors such as mass mailing, self duplication, and registry overwrite without relying on ``pattern files'' that contain ``signatures'' of previously captured samples. The p ...

Keywords: OS execution emulation, code simulation, malicious code detection, static code analysis

12 (How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions
Joris Claessens, Bart Preneel, Joos Vandewalle
February 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 1
Publisher: ACM Press
Full text available: pdf(197.96 KB) Additional Information: full citation, abstract, references, citings, index terms

This article investigates if and how mobile agents can execute secure electronic transactions on untrusted hosts. An overview of the security issues of mobile agents is first given. The problem of untrusted (i.e., potentially malicious) hosts is one of these issues, and appears to be the most difficult to solve. The current approaches to counter this problem are evaluated, and their relevance for secure electronic transactions is discussed. In particular, a state-of-the-art survey of mobile agen ...

Keywords: Mobile agent security, electronic transactions, malicious hosts

13 DRM, trusted computing and operating system architecture
Jason F. Reid, William J. Caelli
January 2005 **Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 ACSW Frontiers '05**
Publisher: Australian Computer Society, Inc.
Full text available: pdf(191.31 KB) Additional Information: full citation, abstract, references, index terms

Robust technological enforcement of DRM licenses assumes that the prevention of direct access to the raw bit representation of decrypted digital content and the license enforcement mechanisms themselves is possible. This is difficult to achieve on an open computing platform such as a PC. Recent trusted computing initiatives namely, the Trusted Computing Group (TCG) specification, and Microsoft's Next Generation Secure Computing Base (NGSCB) aim in part to address this problem. The protection arc ...

14 Security and eliability: Secure and practical defense against code-injection attacks using software dynamic translation
Wei Hu, Jason Hiser, Dan Williams, Adrian Filipi, Jack W. Davidson, David Evans, John C. Knight, Anh Nguyen-Tuong, Jonathan Rowanhill
June 2006 **Proceedings of the second international conference on Virtual execution environments VEE '06**
Publisher: ACM Press
Full text available: pdf(270.13 KB) Additional Information: full citation, abstract, references, index terms

One of the most common forms of security attacks involves exploiting a vulnerability to inject malicious code into an executing application and then cause the injected code to be executed. A theoretically strong approach to defending against any type of code-injection attack is to create and use a process-specific instruction set that is created by a randomization algorithm. Code injected by an attacker who does not know the randomization key will be invalid for the randomized processor effectiv ...

Keywords: software dynamic translation, virtual execution

15 Self-Protected Mobile Agents
J. Ametller, S. Robles, J. A. Ortega-Ruiz
July 2004 **Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems - Volume 1 AAMAS '04**
Publisher: IEEE Computer Society
Full text available: pdf(192.22 KB) Additional Information: full citation, abstract, index terms

In this paper, we present a new solution for the implementation of flexible protection mechanisms in the context of mobile agent systems, where security problems are currently a major issue. In our scheme, agents protect their code and data by carrying their own protection mechanisms. This approach improves traditional solutions, where protection was managed by the platform. The implementation is far from trivial. We have implemented this scheme in the JADE framework, using Java. Any application ...

16 Escrow services and incentives in peer-to-peer networks
Bill Horne, Benny Pinkas, Tomas Sander
October 2001 **Proceedings of the 3rd ACM conference on Electronic Commerce EC '01**